

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:
The premises known as the offices of
Google Inc., 1600 Amphitheatre
Parkway, Mountain View, CA 94043
Account: samgardipe98@gmail.com

CR

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Christian M. Corwin, Special Agent of the Federal Bureau of Investigation (FBI) being duly sworn, states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States, within the meaning of 18 U.S.C. § 2510(7) and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

2. I have been a Special Agent with the FBI since January 2009. I am currently assigned to a criminal squad with the Minneapolis Division of the FBI, Rapid City Resident Agency, and investigate a multitude of Federal criminal violations, including crimes in Indian country on the Pine Ridge Reservation.

3. The information set forth below is based upon my knowledge of an investigation conducted by the FBI and the investigation of other law enforcement agents and officers. I have not included each and every fact

obtained pursuant to this investigation, but have set forth those facts that I believe are essential to establish the necessary probable cause for the issuance of the search warrant.

4. I make this affidavit in support of an application for a search warrant regarding the email account of Palani Bull Bear, samgardipe98@gmail.com, for the time period of July 2, 2017, through July 2, 2018.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a Google, Inc. account that was used to communicate the purchase of the murder weapon, a violation of 18 U.S.C. §§ 1111(a) and 1153 in Attachment A, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1111(a) and 1153 (second degree murder), and which items are more specifically described in Attachment B. The Gmail account is: samgardipe98@gmail.com (also referred to in this affidavit as "Target Account").

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B:
- a. “Chat,” as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
 - b. “Cloud-based storage service,” as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access

is free and readily available to anyone who has an internet connection.

- c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).
- d. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to

restore it.

h. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. “Records,” “documents,” and “materials,” as used herein,

include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

m. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

7. Based on my training and experience and investigation in this case, I have learned the following about Google:

a. Google offers an e-mail service that is available free to Internet users called “Gmail”. Stored electronic communications, including opened

and unopened e-mail for Gmail subscribers may be located on Google's computers.

- b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.
- c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.
- d. When a user sends any e-mail to a Gmail e-mail subscriber the email is stored in the subscriber's "mail box:" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.
- e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, Google retains the email until the user deletes it or exceeds the storage limit.

f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e-mail.

8. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the gmail account and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

9. On June 27, 2018, at approximately 11:18 p.m., an unidentified female called the Oglala Sioux Tribe Department of Public Safety Dispatch (OST DPS) to report a shooting incident in Kyle, SD. Kyle is within the exterior boundaries of the Pine Ridge Reservation.

10. OST DPS law enforcement officers arrived on scene and found the victim, Bryce Red Owl, deceased. Red Owl had three gunshot wounds, one to his chest, another to his wrist and one on his back.

11. The shooter, Palani Bull Bear, fled on foot following the shooting and was located approximately 8 hours later at the Sundance grounds east of Kyle.

12. Your affiant learned that on the morning of June 28, 2018, FBI SA Kevin Seymore and Bureau of Indian Affairs Special Agent Molanna Clifford interviewed Bull Bear in Kyle.

13. Bull Bear waived his Miranda rights and advised SA Seymore that he encountered Red Owl and at least one other male on horseback near Angel's in Kyle. (This male with Red Owl was later determined to be Tolin Gregg). Bull Bear was traveling with his cousin, Antwan Bull Bear and cousin's girlfriend, simply identified as "D," at the time. Bull Bear advised SA Seymore that Red Owl and Gregg were drunk and acting stupid.

14. Bull Bear advised SA Seymore that the men on horseback appeared unarmed and that they continued to act drunk and stupid. Bull Bear told his cousin and his cousin's girlfriend to go inside their house while he approached the men on horseback. Bull Bear advised SA Seymore that he got mad at the men on horseback following a verbal altercation.

15. Bull Bear informed SA Seymore that he took out his gun, a .40 caliber Springfield XD40 semiautomatic pistol, and fired two rounds in the air. Bull Bear advised SA Seymore that the men on horseback appeared to be coming in his direction and that he started running down a "dark alleyway." Your affiant learned from SA Seymore that after catching up to Bull Bear, Red Owl attempted to grab Bull Bear's shirt near the shoulder area from on top of the horse. Bull Bear fired at least two rounds and admitted to striking Red Owl in the torso.

Your affiant learned from SA Seymore that after being hit by the bullet, Red Owl slumped forward and fell off his horse.

16. Bull Bear told SA Seymore that after the shooting he fired several rounds in the direction of Tolin Gregg.

17. Your affiant learned that following the shooting, Bull Bear fled on foot.

18. Your affiant learned that Bull Bear claimed he fell over a barbed-wire fence and may have lost the firearm in a field.

19. Bull Bear told SA Seymore that at some point he may have set down the gun and that he may have left the gun with the hat. Your affiant learned that Bull Bear advised SA Seymore that during the shooting he was wearing a black "L.A. Kings" hat.

20. Your affiant is aware that SA Clifford used a metal detector in the area in which Bull Bear claims to have either lost or set the gun down. SA Clifford did not find the gun.

21. On July 2, 2018, your affiant learned that BIA Special Agents Ted Thayer and Darrell Robinson interviewed Bull Bear at the Pine Ridge Jail in Pine Ridge, SD on June 29, 2018. Your affiant learned that Bull Bear purchased the firearm from a third party based on an advertisement on Armslist.com. Armslist.com is an online marketplace similar to Craigslist.com in which users can exchange firearms and buy and sell firearms. Bull Bear stated that he communicated with the seller of the gun via email. Your affiant learned that Bull

Bear provided the email samgardipe98@gmail.com to Agents Thayer and Robinson. "Sam" is Bull Bear's middle name and "98" is the year of Bull Bear's birth. "Gardipe" is Bull Bear's father's last name.

22. Your affiant learned that Bull Bear advised BIA agents that he used his gmail account to create a username and account on Armslist.com and that he purchased the Springfield XD40 around February of 2018.

23. Your affiant is requesting a search warrant of the gmail account to determine the specifics and serial number of the gun and to determine if it was in fact purchased from Armslist.com.

24. By searching the account, your affiant will be able to verify the communication and the nature of the communication between Bull Bear and the potential seller of the firearm.

25. The target account is samgardipe98@gmail.com.

26. Bull Bear is currently an enrolled member of the Oglala Sioux Tribe.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to

locate the items described in Section II of Attachment B.

JURISDICTION

28. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

29. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the following account: samgardipe98@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Google, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for

the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Google, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

30. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

31. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned,

maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google, Inc. account, listed in Attachment A has been used for the purpose of communicating with the suspect involved in a violation of 18 U.S.C. §§ 1111(a) and 1153, which items are more specifically described in Attachment B. There is probable cause to believe that Bull Bear, user of the Gmail account, communicated with the potential seller of the firearm that was used to commit a homicide in the District of South Dakota. The account is the subject of this warrant affidavit. The accounts is samgardipe9820@gmail.com.

33. Law Enforcement agents will serve the warrant on Google, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

34. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. via the internet and to allow Google, Inc. to copy the data outside of

this agent's presence.

Dated: 7/5/2018

SA Christian Corwin
Special Agent Christian Corwin
Federal Bureau of Investigation

SUBSCRIBED and SWORN to in my presence

this 5th day of July, 2018.

Daneta Wollmann
DANETA WOLLMANN
U.S. MAGISTRATE JUDGE